Towards Better Security Decisions: Applying Prospect Theory to Cybersecurity

Leilei Qu
Cheng Wang
Ruojin Xiao
Renmin University of China
Beijing, P. R. China
llqu@ruc.edu.cn
rucwangc@ruc.edu.cn
ruojinx@ruc.edu.cn

Jianwei Hou
Wenchang Shi*
Bin Liang
Renmin University of China
Beijing, P. R. China
houjianwei@ruc.edu.cn
wenchang@ruc.edu.cn
liangb@ruc.edu.cn

*Corresponding author

ABSTRACT

Normal users are usually not good at making decisions about cybersecurity, being easily attacked by hackers. Quite a few tools have been devised and implemented to help, but they can not balance security and usability well. To solve the problem, this paper explores the application of prospect theory to security recommendations. We conducted online surveys (n=61) and a between-subjects experiment (n=106) in six conditions to investigate the issues. In the experiment, we provided different security recommendations about two-factor-authentication (2FA) to participants in different conditions and recorded their decisions about enabling it. Results show that participants in the condition "Disadvantage" were willing to adopt 2FA the most. The findings indicate that showing disadvantages can be useful to persuade users into better security decisions.

CHI'19 Extended Abstracts, May 4–9, 2019, Glasgow, Scotland UK

ACM ISBN 978-1-4503-5971-9/19/05.
https://doi.org/10.1145/3290607.3312782

KEYWORDS
Security decisions; Prospect theory; Security recommendations; Usable security

What is Prospect Theory? [12]

Key Point: Given a single decision problem and several corresponding options, the relative attractiveness of those options varies when the problem is framed in different ways.

Embodiment:

(1) Pseudo-certainty effect: Protection and defense schemes such as insurance should appear more attractive when it is described as the elimination of one single kind of risk than when it is described as a reduction of the overall risk.

(2) Reference-dependent preference: A difference between two options will become more obvious when it is framed as a disadvantage of one option rather than as an advantage of the other one.

INTRODUCTION

Recently, it has been widely recognized that human, rather than technical issues, is the weakest link in cybersecurity [15]. Many cybersecurity incidents were mainly caused by human factors. Take RockYou Hack [3] as an illustrative example, the faults of both administrators and users can be found in that event. Apparently, human problems cannot get settled merely by technical methods [15]. Just as what Waldrop et al. [15] have claimed, we cannot expect digital walls to keep everything evil outside. Instead, we have to look inside to find problems on the human side [15].

Studies on human behaviors have shown that most people are weak in "doing the right thing" in cyberspace [10, 11, 16]. People are used to reusing passwords, clicking unknown links, connecting to the Internet via public free WiFi etc. [10, 15, 16]. By contrast, security researchers and practitioners are always struggling to inform the public of "right" cyber behaviors, yet in vain with users' inobservance [8, 10]. Thus, we must improve the persuasion of our security recommendations.

To our delight, there has been some remarkable work on this problem, most of which is concerned about password creation assistance [6, 13]. They indeed helped a lot, but were still limited to technical areas. Inevitably, they got quite a number of users annoyed [6, 13], which hurts the usability. Actually, poor usability will spur users' psychological resistance. When the resistance accumulates, security will be compromised due to users' uncooperative behaviors [1].

In order to improve the persuasibility of security recommendations, it is natural for us to turn to psychology. Much in-depth research in psychology has been done on human decision-making process. Among all of the excellent work, prospect theory [12] stands out. It focuses on helping people with risk decision, widely applied to cases like insurance and marketing. In our research, we pay more attention to the *Pseudo-certainty effect* and the *Reference-dependent preference*. More details about them are presented in the sidebar. Some researchers [7] have realized the potential value of prospect theory for cybersecurity, but few have experimented to explore the feasibility and specific methods. Thus, in order to fill the gap, we explore the application of prospect theory in guiding people towards better security decisions through elaborate experiments.

RELATED WORK

Factors account for security behaviors

The process of human decision-making and behaving is tangled. Sawaya et al. [11] discovered the diversity of security awareness degrees of people from different culture. As for phishing training, it was shown that people tended to follow facts-and-advice from experts or narrative stories from close peers [16]. Similarly, Chinasson et al. [2] concluded that a click-based graphical passwords mechanism could balance security and usability in the short-term with the memory cueing it provided. Moreover, Redmiles et al. [9] indicated users' bounded-rationality in face of cybersecurity decisions .

Hypotheses

$H0_1$. There is no significant difference in the security decisions made by participants across all groups.

$H0_2$. There is no correlation between the security decisions made by participants and the different treatments.

Security Decision Problem Examples

Decision 1. Choose between: (n=11)

A. Enable 2FA to reduce the risk of privacy leakage.

B. Sign in only with the password.

Decision 2. Choose between: (n=18)

A. Enable 2FA to eliminate the risk of password-guessing attacks.

B. Sign in only with the password.

Decision 3. Choose between: (n=16)

A. Enable 2FA.

B. Ignore potential risks of password-guessing attacks and sign in only with the password.

Table 1: Results of Online Surveys

	A*	B*
Decision 1	45.5%	54.5%
Decision 2	77.8%	22.2%
Decision 3	56.3%	43.8%

*: A and B refer to options A and B in the above security decision problem examples, respectively.

Guidance towards better security decisions

Researchers have attempted to use psychological theories to guide people towards better security decisions. People with different cognitive styles adopted different tactics when creating graphical passwords, which could be utilized to design an assistive mechanism to improve their performance in creating strong passwords [5]. According to Wilson et al. [17], people's experiences in various temperature and attitudes towards various warning degrees could be associated to strengthen the stimulus of security warnings, making them more willing to follow the advice. As for password management, Kankane et al. [4] chose nudge theory as their helper in a between-subjects experiment. Actually, their work is not sufficient to change users' behaviors [4] but indicates some directions to further the study. That is why we choose prospect theory [12] as our nudge. Actually, experiment results have shown that we can induce substantial changes in user behaviors.

RESEARCH OVERVIEW

Participants in our study were recruited via social media posts. They were randomly grouped to receive different treatments, which meant different security recommendations. Then we formed two null hypotheses (see "Hypotheses" in the sidebar). In order to test the hypotheses, we conducted two kinds of studies: online surveys and a field experiment, for which we compensated participants RMB ¥5 and RMB ¥10, respectively. Actually, through online surveys, appropriate phraseology of security recommendations were discovered, which facilitated the field experiment.

ONLINE SURVEY

Methodology

In our surveys, the reproduction of surveys by Tversky and Kahneman [12] and a survey queried participants' decisions about cybersecurity (examples are illustrated by "Security Decision Problem Examples" in the sidebar) were carried out successively. By reproduction, we aimed to test the applicability of prospect theory in China and obtain an appropriate description of security decision problems. According to Sawaya et al. [11], we had to be careful with phraseology and translation. Thus, the process of testing and refining was repeated until satisfactory results like what Tversky and Kahneman [12] had obtained were accessed. With the consideration that security recommendations presented risk-aversion measures like insurance [12], we used the phraseology we had obtained in the reproduction to design security decision problems and then surveyed users' responses to them.

Findings & Discussions

In the final survey about security decision problems, we had 61 participants, 45 of which passed the attention check question (an image recognition test). We discovered that the reproduction and the

Prompt Design

Control : Whether to enable 2FA?
A. Yes.
B. No.

Normal: Considering that your game account is at risk, we recommend that you enable 2FA for it. Whether to enable?
A. Yes.
B. No.

Nudge: Your personal information could be at risk for hackers to exploit. At this moment, thousands of hackers are combing the Internet for personal data [4]. Enabling 2FA could prevent your data from reaching them. Whether to enable?
A. Yes.
B. No.

Reduction: Considering that your account is at risk, we recommend that you enable 2FA for it. Please choose between:
A. Enable 2FA to reduce the risk of privacy leakage.
B. Sign in only with the password.

Elimination: Considering that your account is at risk, we recommend that you enable 2FA for it. Please choose between:
A. Enable 2FA to eliminate the risk of password-guessing attacks.
B. Sign in only with the password.

Disadvantage: Considering that your account is at risk, we recommend that you enable 2FA for it. Please choose between:
A. Enable 2FA.
B. Ignore potential risks of password-guessing attacks and sign in only with the password.

survey of security decisions showed similar characteristics. The results are presented in Table 1. From the table, we can see that (1) participants preferred the elimination of a certain risk to the reduction of the overall risk, and (2) security precautions did not appear more attractive when expressed as a disadvantage of not taking than an advantage of taking. Actually, (2) is surprising for it is opposite to the embodiment of *Reference-dependent preference* [12]. Thus, we went on to test it further.

FIELD EXPERIMENT

Methodology

Due to the popularity of WeChat in China and even around the world, we utilized its Mini Program to conduct a between-subjects online field experiment. In order to get participants' true responses, we designed an interesting game named "Pick the Stronger". In the game, participants were shown ten pairs of similar passwords and required to pick the stronger one of each pair. Before the game started, a prompt about whether to enable 2FA popped up and required participants to make a decision.

Participants were randomly assigned to six different conditions automatically by the game program, which were "Control", "Normal", "Nudge", "Reduction", "Elimination" and "Disadvantage" (see "Prompt Design" in the sidebar). The first three were associated with prompts with no explanations, simple explanations as common practice and the salience nudge as designed by Kankane et al. [4], respectively. The remaining three were designed according to security decision problems of our online surveys, with prospect theory [12] embedded. It is worth mentioning that the passwords in the game were created based on 27 hypotheses, a modification of what was designed by Ur et al. [14], and the strength of the passwords was calculated by the tool implemented by Ur et al. [13].

In addition, a questionnaire queried participants' demographics and feelings about the prompts was placed at the game exit, but merely as an option.

Findings & Discussions

The field experiment was conducted to explore whether we could induce substantial changes of user behaviors about cybersecurity. We had 106 participants in six conditions (see Figure 1). Participants of different conditions showed significantly different decision tendencies (see Figure 2). It can be discovered from Figure 2 that participants in the condition "Disadvantage" were willing to adopt 2FA the most. It was shown by a Chi-square test of independence that there was a significant difference on the security decisions made by participants across all conditions ($\chi^2(10) = 17.245$, $p = 0.003$, Fisher's exact test), which implied the correlation between decisions and security recommendations of different phraseology as well. Thus, we could reject the null hypotheses $\mathbf{H0}_1$ and $\mathbf{H0}_2$. In addition, pairwise comparisons among "Reduction", "Elimination" and "Disadvantage" implied the embodiment of prospect theory. For example, the comparison between "Elimination" and "Disadvantage" indicated

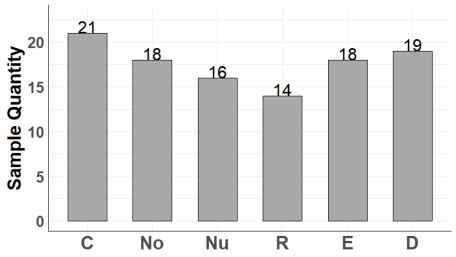

Figure 1: Participant distribution (conditions with initial letters)

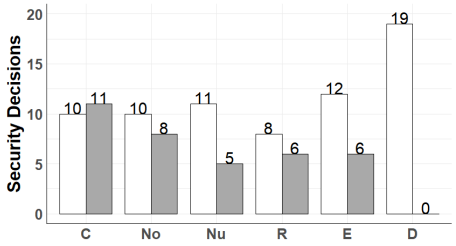

Figure 2: Security decisions (The blank area for "Yes", the shaded area for "No")

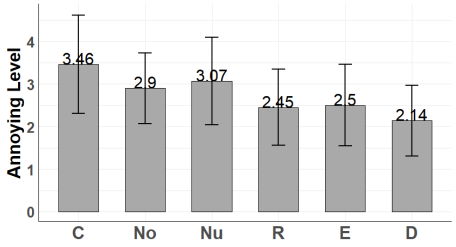

Figure 3: Means of annoying levels and associated error bars

participants' *Reference-dependent preference*—the difference between adopting 2FA and not adopting it loomed larger under the expression of "disadvantage" than "advantage".

Furthermore, with respect to the embodiment of the *Reference-dependent preference*, it is discovered that the results of the survey and the field experiment appear opposite. We consider it is because participants can not experience a real worry about the risk of privacy leakage without a real scenario.

76 out of 106 participants offered responses to the questionnaire, 68 of which were valid. Among these valid ones: (1) 34 females, 33 males, 1 others. (2) 91.2% were between 18-29 years old. (3) participants with technical background (n=21) did not make better decisions than participants without (n=47). An example of the results is presented in Figure 3. It is discovered that the "Disadvantage" is the least annoying for participants. There were some other questions like "I think the information the prompt provided was useful" and "My decision was influenced by the prompt". Their choices were reported via a Five-point Likert Scale (1 = Totally Disagree, 5 = Totally Agree; M = 3.01, 2.82; SD = 0.98, 1.01). To avoid bias, we did not mention the prompt before the game. It is surprising that only two realized our true purpose even if several questions mentioned the prompt.

CONCLUSIONS & FUTURE WORK

This paper discusses the use of prospect theory to nudge user into desirable security decisions. To study the feasibility and specific methods, we conducted online surveys and a field experiment. Results indicate that showing disadvantages can be useful to nudge participants. These findings can help effectively improve the persuasion of security recommendations, guiding users towards better security decisions. The findings may also be useful to mitigate social engineering attacks to some extent.

In the future, we are to test the correlations between security awareness and decisions. Moreover, other decisions such as whether to click an unknown link are also within our consideration.

ACKNOWLEDGMENTS

This work was supported by the National Natural Science Foundation of China under grant No.61472429.

REFERENCES

[1] Anne Adams and Martina Angela Sasse. 1999. Users are not the enemy. *Commun. ACM* 42, 12 (1999), 40–46. https://doi.org/10.1145/322796.322806

[2] Sonia Chiasson, Alain Forget, Elizabeth Stobert, Oorschot P. C. van, and Robert Biddle. 2009. Multiple password interference in text passwords and click-based graphical passwords. In *CCS '09 Proceedings of the 16th ACM conference on Computer and communications security (CCS '09)*. ACM, New York, NY, USA, 500–511. https://doi.org/10.1145/1653662.1653722

[3] Nik Cubrilovic. 2009. RockYou Hack: From Bad To Worse. https://techcrunch.com/2009/12/14/rockyou-hack-security-myspace-facebook-passwords/.

[4] Shipi Kankane, Christen Buckley, and Carlina DiRusso. 2018. Can We Nudge Users Toward Better Password Management? An Initial Study. In *CHI EA '18 Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems*

(CHI EA '18). ACM, New York, NY, USA, LBW 593: 1–6. https://doi.org/10.1145/3170427.3188689

[5] Christina Katsini, Christos Fidas, George E. Raptis, Marios Belk, George Samaras, and Nikolaos Avouris. 2018. Influences of Human Cognition and Visual Behavior on Password Strenth during Picture Password Composition. In *CHI '18 Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18)*. ACM, New York, NY, USA, Paper 492: 1–12. https://doi.org/10.1145/3173574.3173661

[6] Saranga Konmanduri, Richard Shay, Lorrie Faith Cranor, Cormac Herley, and Stuart Schechter. 2014. Telepathwords: Preventing Weak Passwords by Reading Users' Minds. In *SEC'14 Proceedings of the 23rd USENIX conference on Security Symposium (SEC'14)*. USENIX Association, Berkeley, CA, USA, 591–606. https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/komanduri

[7] Shari Lawrence Pfleeger and Deanna D. Caputo. 2012. Leveraging behavioral science to mitigate cyber security risk. *Computers and Security* 31, 4 (2012), 597–611. https://doi.org/10.1016/j.cose.2011.12.010

[8] Elissa M. Redmiles, Sean Kross, and Michelle L. Mazurek. 2016. How I Learned to be Secure: a Census-Representative Survey of Security Advice Sources and Behavior. In *CCS '16 Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS '16)*. ACM, New York, NY, USA, 666–677. https://doi.org/10.1145/2976749.2978307

[9] Elissa M. Redmiles, Michelle L. Mazurek, and John P. Dickerson. 2018. Dancing Pigs or Externalities?: Measuring the Rationality of Security Decisions. In *EC '18 Proceedings of the 2018 ACM Conference on Economics and Computation (EC '18)*. ACM, New York, NY, USA, 215–232. https://doi.org/10.1145/3219166.3219185

[10] Robert W. Reeder, Adrienne Porter Felt, Sunny Consolvo, Nathan Malkin, Christopher Thompson, and Serge Egelman. 2018. An Experience Sampling Study of User Reactions to Browser Warnings in the Field. In *CHI '18 Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18)*. ACM, New York, NY, USA, Paper 512: 1–13. https://doi.org/10.1145/3173574.3174086

[11] Yukiko Sawaya, Mahmood Sharif, Nicolas Christin, Ayumu Kubota, Akihiro Nakarai, and Akira Yamada. 2017. Self-Confidence Trumps Knowledge: A Cross-Cultural Study of Security Behavior. In *CHI '17 Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. ACM, New York, NY, USA, 2202–2214. https://doi.org/10.1145/3025453.3025926

[12] Amos Tversky and Daniel Kahneman. 1981. The Framing of Decisions and the Psychology of Choice. *Science* 211, 4481 (1981), 453–458. http://www.jstor.org/stable/1685855

[13] Blase Ur, Felicia Alfieri, Maung Aung, Lujo Bauer, Nicolas Christin, Jessica Colnago, Lorrie Faith Cranor, Henry Dixon, Pardis Emami Naeini, Hana Habib, Noah Johnson, and William Melicher. 2017. Design and Evaluation of a Data-Driven Password Meter. In *CHI '17 Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. ACM, New York, NY, USA, 3775–3786. https://doi.org/10.1145/3025453.3026050

[14] Blase Ur, Jonathan Bees, Sean M. Segreti, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2016. Do User's Perceptions of Password Security Match Reality?. In *CHI '16 Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16)*. ACM, New York, NY, USA, 3748–3760. https://doi.org/10.1145/2858036.2858546

[15] M. Mitchell Waldrop. 2016. How to Hack the Hackers: The Human Side of Cybercrime. *Nature* 533, 7602 (2016), 164–167. https://doi.org/10.1038/533164a

[16] Rick Wash and Molly M. Cooper. 2018. Who Provides Phishing Training? Facts, Stories, and People Like Me. In *CHI '18 Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18)*. ACM, New York, NY, USA, Paper 492: 1–12. https://doi.org/10.1145/3173574.3174066

[17] Graham Wilson, Harry Maxwell, and Mike Just. 2017. Everything's Cool: Extending Security Warnings with Thermal Feedback. In *CHI EA '17 Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems (CHI EA '17)*. ACM, New York, NY, USA, 2232–2239. https://doi.org/10.1145/3027063.3053127